06 | 网络：先有去中心化还是先有点对点？

2021-08-02 赵铭

《说透区块链》 课程介绍 >

讲述：赵铭
时长 15:56 大小 14.60M

你好，我是赵铭。

你知道么？没有互联网，我们每个人都是信息孤岛，只能过着单机生活。我们现在很方便就能获取信息，正是依赖互联网这样的信息传递纽带。而我们常说的信息量爆炸，也是因为现在的信息并不依赖特定的源头，而是千千万万个普通人独立自主生产出来的。

其实，区块链中的网络也没什么不同，每个节点都是独立平等的信息源头。前面我曾经说过“点对点网络是搭建区块链建筑的混凝土”，但这个网络到底是怎样支撑区块链的呢？

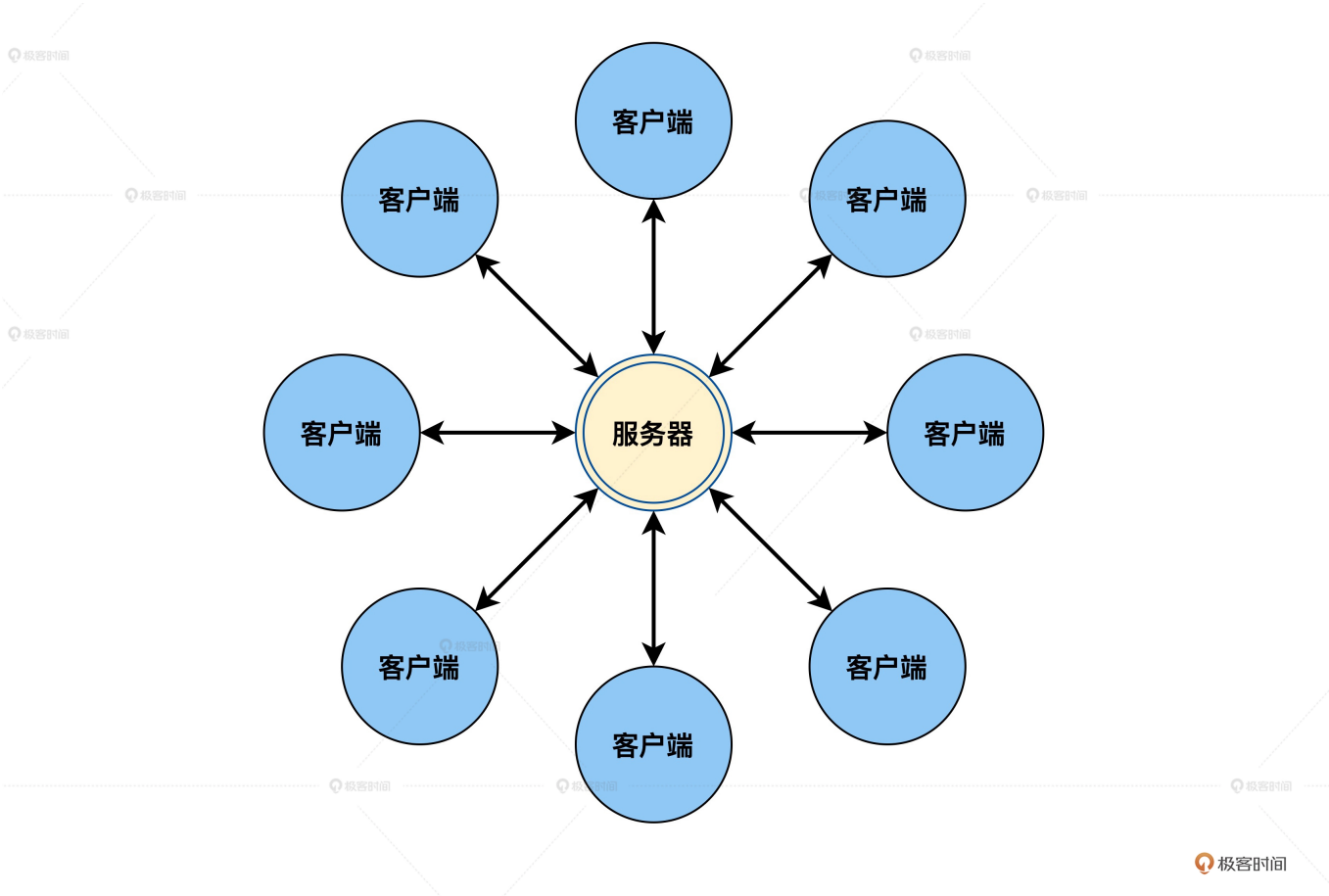
想要理解这背后的原理，我们可以从这样一个问题开始：**到底是因为区块链需要去中心化，才选择了点对点网络技术？还是因为点对点网络的启发，区块链才有了去中心化特性呢？**

这是一个类似于是先有鸡还是先有蛋的无解思辨，我想将这个问题先留给你，希望你在学完这一讲之后，能有自己独立的理解。不过不管你是什么观点，这个问题里有两个关键词我们先要搞清楚，它们分别是点对点网络模型和去中心化。我们先从网络模型说起。

网络模型

为什么区块链会采用点对点网络模型作为节点间数据传递的纽带呢？要想真正搞懂这种思路，我们做个对比。

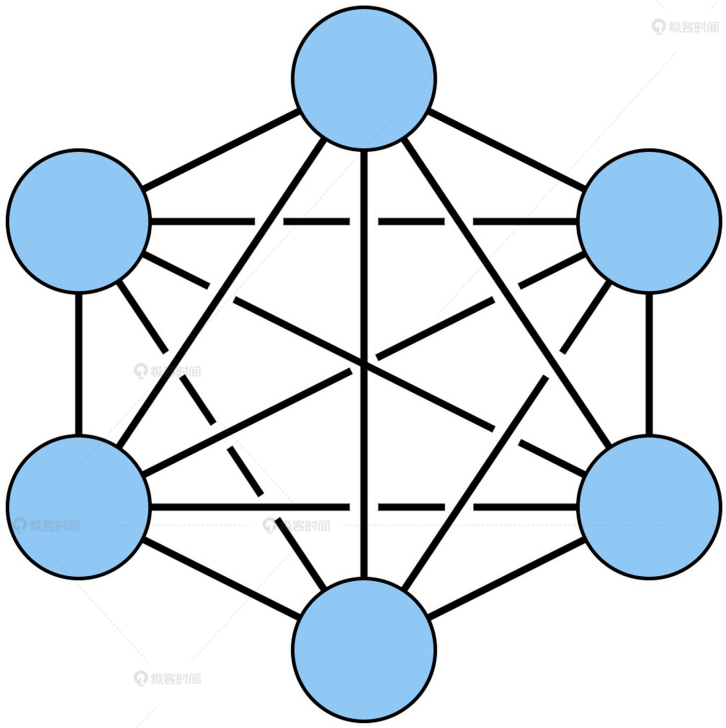
不管是点外卖还是买车票，在日常工作生活中，我们接触的大部分网络应用架构都是**客户端 - 服务器模型**。这个模型的运行机制是这样的：各个客户端向服务器发送请求，而服务端负责接收并处理请求，最终给客户端返回处理结果。为了让你直观理解，我还画了一张示意图。



中心化网络示意图

结合示意图，我们可以清晰认识到这是一个中心化的网络架构，其服务能力完全取决于中心的服务器，如果中心服务器因意外导致宕机，那整个服务就瘫痪了。整个应用的可用性仅依赖于服务器的活性，与客户端无关。

而点对点网络则完全不同，它是一种分布式的网络架构，并不存在单一的中心服务器。网络中每个节点的权利与义务都是一致的。每个节点都拥有向网络中其他节点发起请求的权利，同时也有着必须响应其他节点请求的义务。



点对点网络示意图

你可以想一下，节点权利与义务的对等意味着什么呢？这代表**点对点网络的可用性是随着节点数的增多而增强的，网络的运行并不依赖任何单一节点，节点可以任意地加入或者退出。**即使一些节点宕机或者遭受攻击，只要还有正常运行的节点，整个系统依旧可以照常运作。

怎么形象地理解二者的区别呢？我们拿银行系统来举例，如果按现有的中心化架构，有一天银行网点大面积停摆，不对外提供服务。原因可能很简单，排除网络的干扰，大概率是银行的总机房出现了问题，这就是中心化架构可能出现的单点故障。

而区块链架构则不同，一家银行就相当于一个区块链网络，每一个银行网点代表一个区块链节点，一个节点无法对外提供服务，我们可以随时切换另一个节点，一两个节点的问题不影响整个网络。当然，这个例子描述得非常极端粗暴，只是为了帮你理解，真正的银行系统架构不会这么脆弱。

我们之前反复提过，区块链是一种摒弃可信任第三方的技术手段，而中心化网络架构俨然就是为第三方中介量身打造。区块链需要摆脱中心节点的束缚，将权利与义务分散到每个节点，而采用点对点网络模型，正好顺应了这一思想。

网络拓扑

从某种角度来说，不管是先有鸡还是先有蛋，点对点网络与区块链都是相互成就的 CP 组合。

前面课程中，我说过区块链的去中心化是相对去中心化，而绝对去中心化只是一个理想状态，如果对应到点对点网络，这其实是由点对点网络的拓扑结构决定的。怎么理解这种对应关系呢？

只有一个节点的网络实质就是中心化网络，此时区块链表现为中心化。而如果网络中所有的节点两两之间建立连接，此时点对点网络可以看作是完美对称的，区块链也就表现出绝对去中心化特性。

但如果我们不那么极端，允许点对点网络在这两个极端理论值间左右摇摆，就会发现**区块链网络会一直处于中心化与绝对去中心化之间的动态平衡之中，而对去中心化程度的考量主要依托于对点对点网络拓扑结构的选择**。

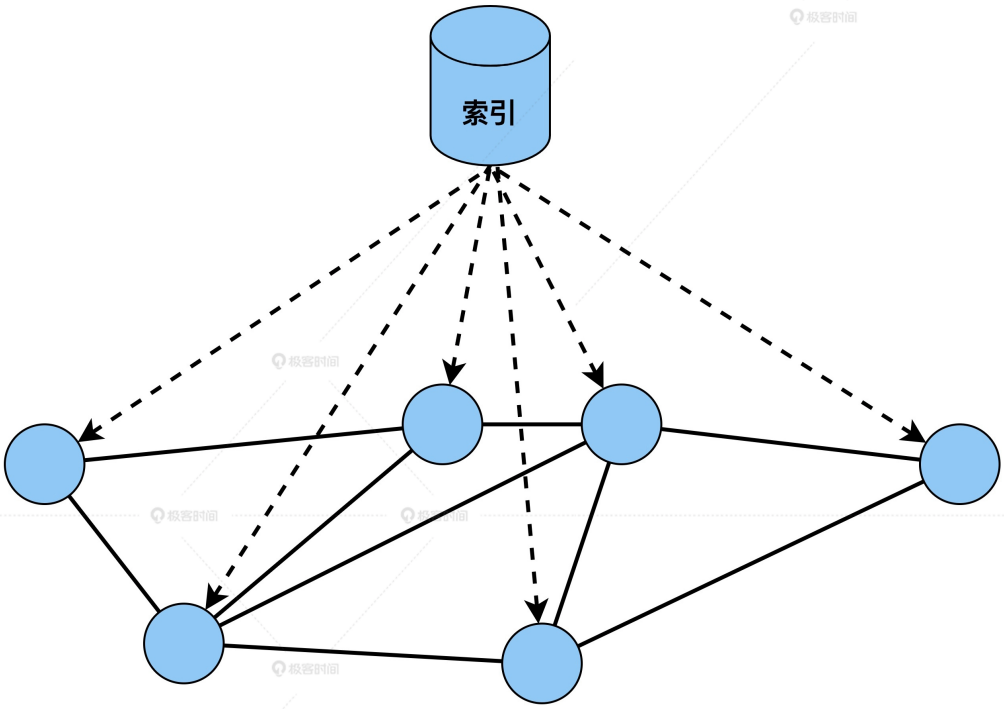
这么说你可能还是有点懵，别担心，我们来一起理一理这中间的逻辑。相比中心化网络，点对点网络虽然优势明显，但它的不足也同样明显，那就是新的节点加入网络之前，必须知道至少一个已经存在于网络里的节点，不然这个新节点跟整个网络就是脱钩的。

这点非常容易理解：在中心化网络中，客户端要想让服务器响应自己的请求，必须先将自己的请求发送到服务器，而这就要求客户端知道服务器在哪，就像你上网必须要知道网址一样。而点对点网络则不一样，所有节点互为服务器客户端，因此节点必须知道其他节点的地址，才能加入网络。

对节点发现机制处理的不同，也就形成了不同的网络拓扑结构，下面我分别为你分析一下。

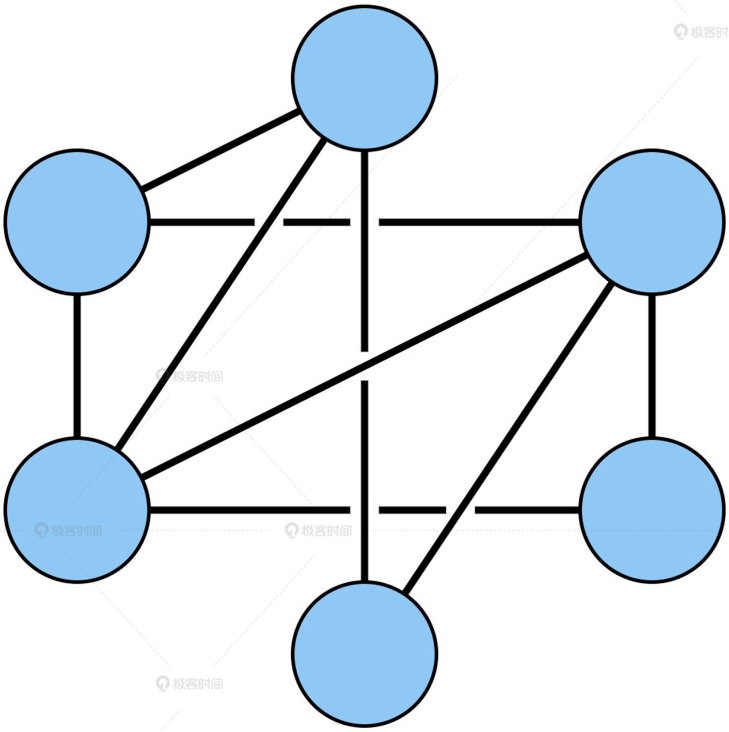
第一种结构是**引入了一个中心索引节点**，用来保存其他所有节点的接入信息。新节点的加入首先将自身信息传入中心节点，从而换取已在网络中其他节点的连接信息，随后与其他

节点组成点对点网络，这种结构与我们使用搜索引擎进行信息检索是类似的，但存在单点故障的可能性，一旦中心索引节点宕机，新节点将无法加入网络。



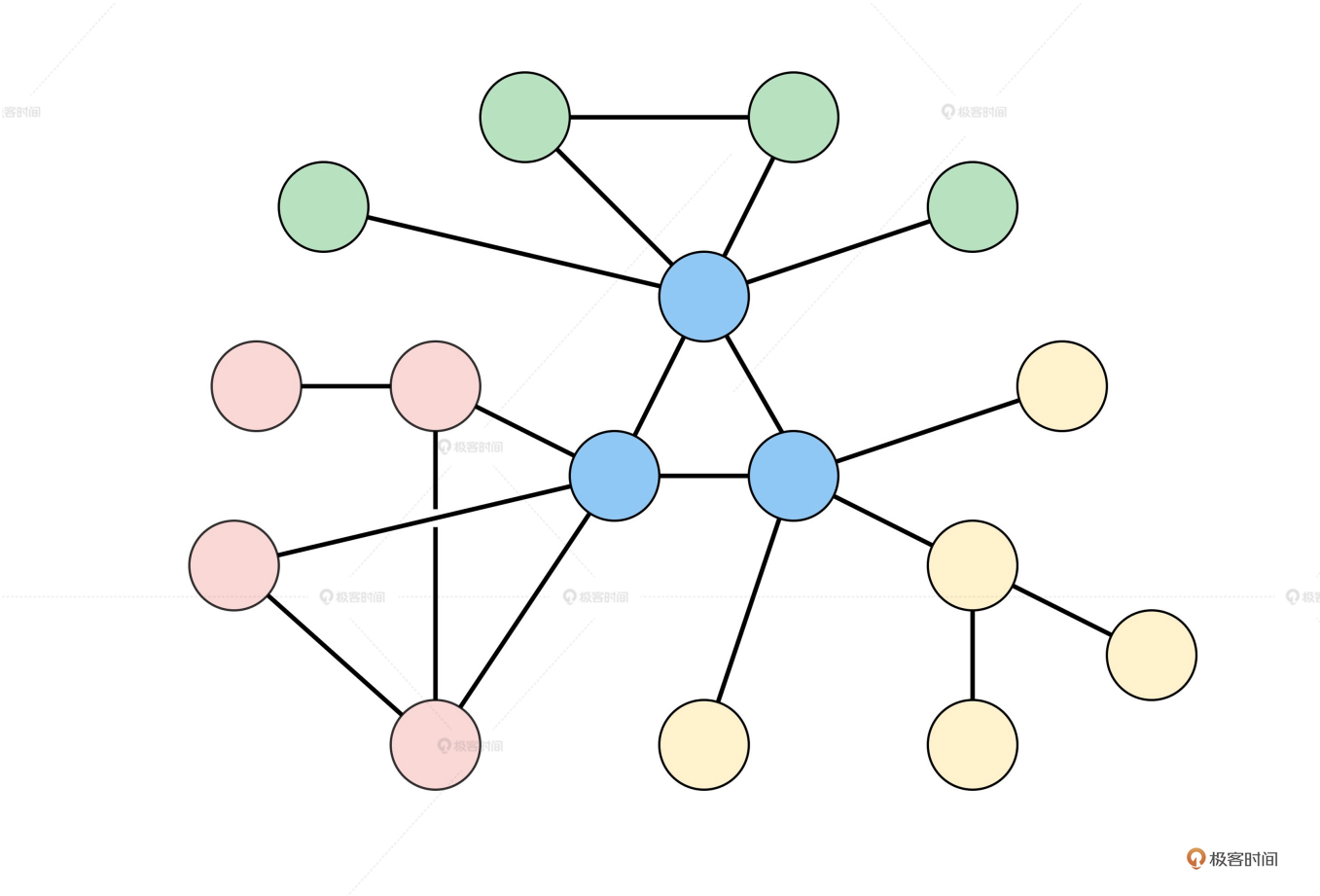
中心索引网络拓扑示意图

第二种结构你可以理解成一种**无为而治**的结构。新节点选择连接一个已存在网络中的节点，被连接的节点可以告知新节点它连接的其他节点信息，这样新节点可以随机选择再连接到其他节点，这样就形成了一张没有规律的网络拓扑结构。



无为而治网络拓扑示意图

而第三种结构则融合了前两种结构的特点，整个网络由多个种子节点形成主干网络，而其他普通节点则连接到某个种子节点，这样就形成了**整体分散局部集中的混合结构**。



混合网络拓扑示意图

最后一种网络拓扑是结构化的，它跟上面讲的三种拓扑不同，节点间的连接遵循某种算法，组成了一种**有序的结构化网络**，比如树形网络结构。大多数结构化网络的算法都是基于**分布式哈希表**算法实现的，这是一种用于在大量节点的系统中快速定位目标节点的索引算法，具体原理你可以参考扩展阅读。

区块链网络拓扑

了解了这 4 种网络拓扑结构之间的差异，那区块链中到底是如何组织节点拓扑的呢？纵观前面说的比特币跟以太坊网络，你会发现它们的选择是有差异的。

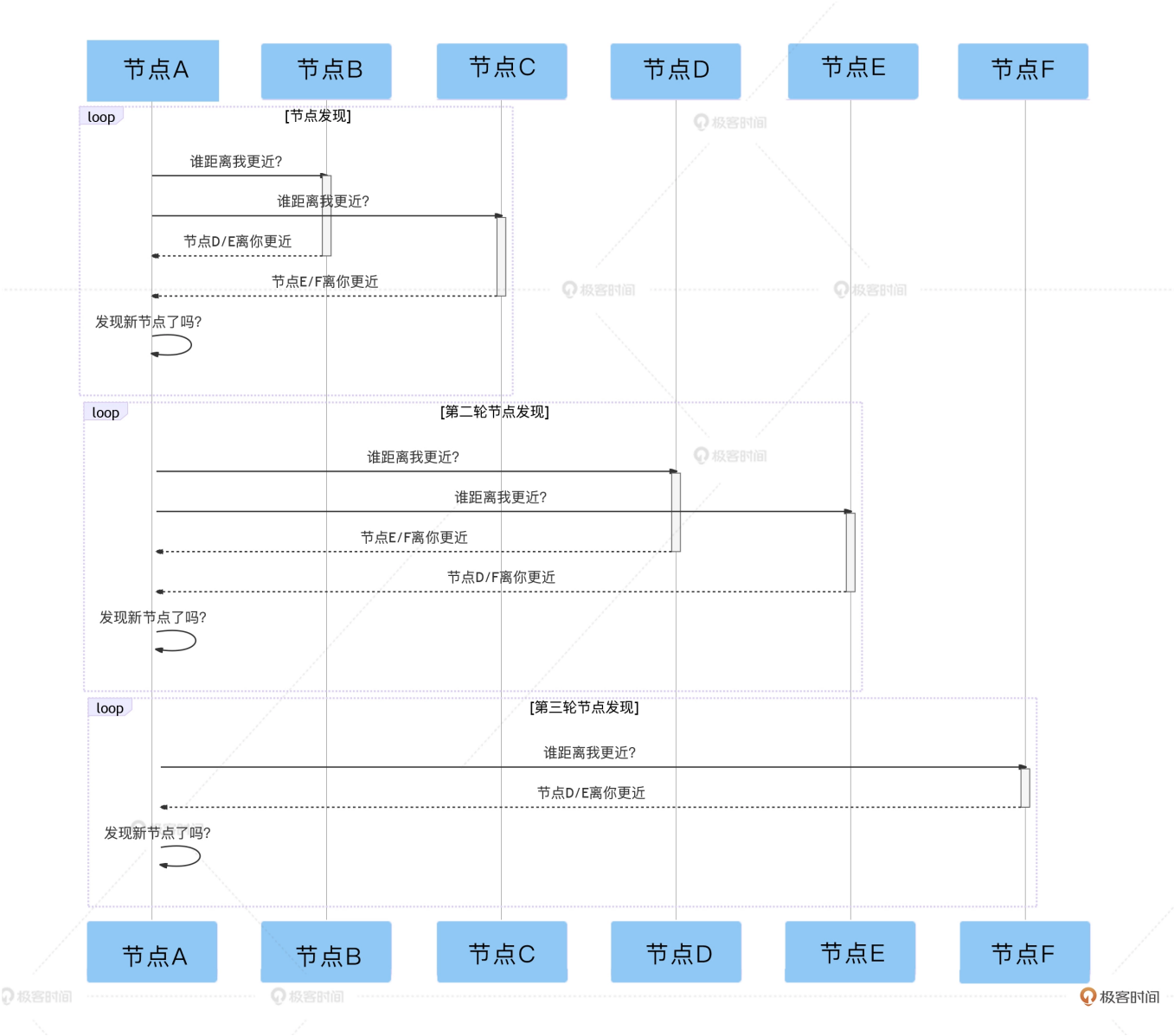
比特币采用的是类似于**混合型**的网络拓扑结构，一个新节点的加入需要给节点指定几个已在比特币网络中的相邻节点信息，可以是普通节点，也可以是种子节点。

当建立节点间连接以后，新节点将自身信息发送给相邻节点，相邻节点再将新节点的信息依次转发给它们各自的相邻节点，从而保证了新节点信息在网络中被广泛传播。新节点也可以从相邻节点获取该节点的相邻节点信息，从而选择性地连接更多节点，增强节点自身与整个网络连接的稳定性。

比特币中的点对点网络相对简单，也更容易理解，但信息传递的效率不高，并且对网络带宽的负载要求较高，这点你看完后面交易的扩散过程就能明白了。

而以太坊的选择则不太一样，使用的是结构化网络拓扑，打造这种结构，离不开基于分布式哈希表思想的Kademlia 算法（后面简称 Kad 算法）。虽然 Kad 算法的原理比较复杂，但如果你能先理解它干了什么事，就会大大降低学习难度。

简单来讲，Kad 算法定义了一种节点间距离计算的方法，用于新节点的发现。那具体怎么计算呢？我们接着往下看。



Kad算法示意图

节点 A 首先从自身存储节点信息的 K 桶中找出 2 个与自己距离最近的节点，之后请求这 2 个节点，要求他们从各自的 K 桶中分别找出 2 个与节点 A 更近的节点。那么节点 A 最多可以得到 2 × 2 个新节点信息，随后再请求这 2×2 个新节点中距离节点 A 最近的 2 个节

点，让它们再分别返回与节点 A 距离更近的 2 个节点，整个过程持续迭代，直到没有新节点被发现。

通过这种办法，节点 A 只与自己距离最近的节点连接，这保持了以太坊网络中节点的有序。但你需要注意，**节点间的距离是逻辑距离，而并非是物理距离**，也就是说即便两个以太坊节点运行在同一台电脑上，它们之间的逻辑距离也可能无限远，这是算法本身导致的，就比如图中的节点 C 明显离节点 A 更近，但这只是表象，逻辑距离还是 D/E 更近。

通过对比特币以太坊对不同网络拓扑的选择，我们可以发现，区块链中选择网络结构是没有定式的，没有唯一标准。

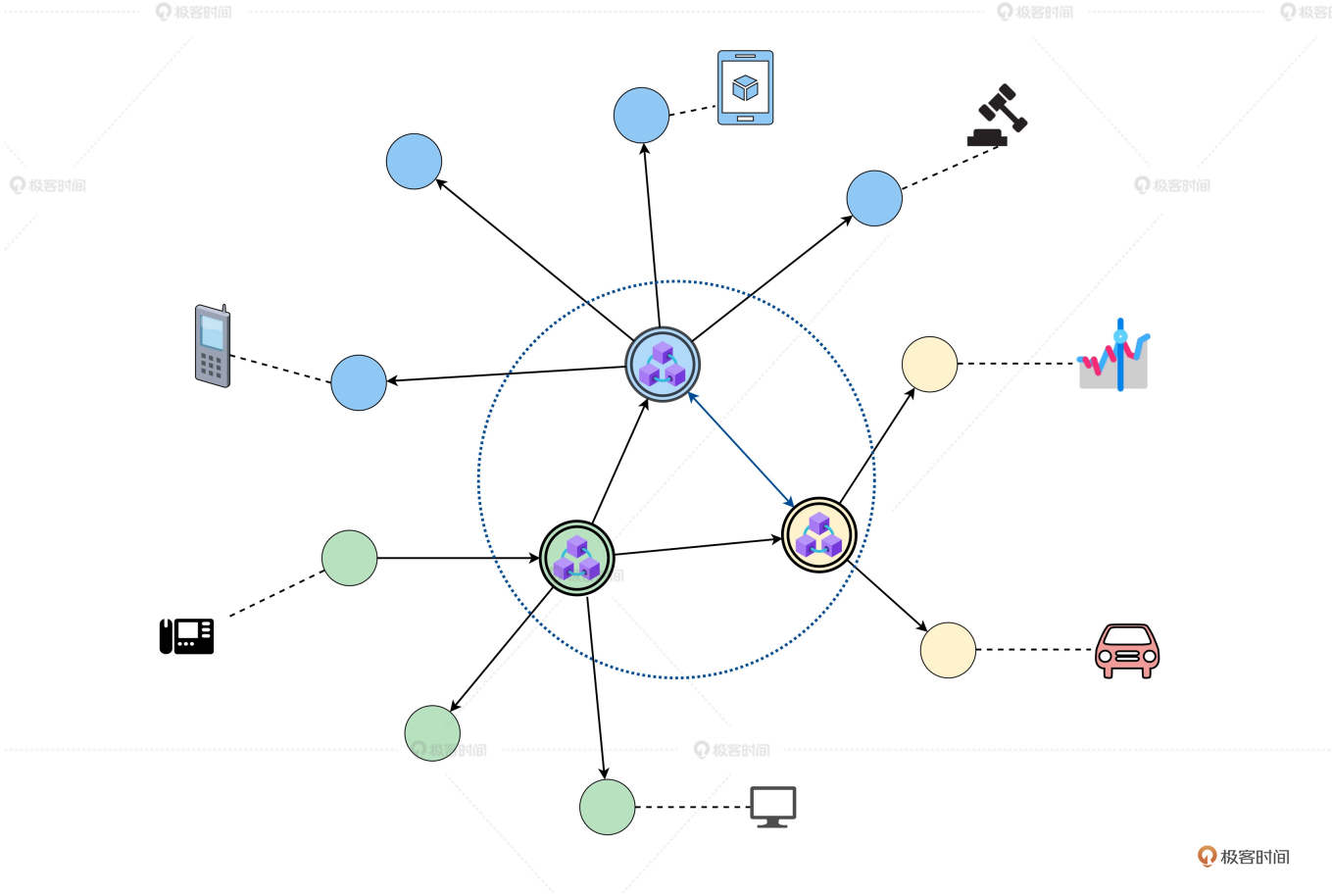
如果你熟悉联盟链技术体系，就会发现联盟链对点对点网络的重视程度不如公链，主要有两方面原因，一方面联盟链的节点是确定的，很少出现随时加入，随时退出的需求；另一方面联盟链节点个数比较少，并不需要节点发现机制引导新节点的加入。

交易的扩散

有了前面基础知识的铺垫，我们终于可以将交易通过网络流动起来了，接下来我们通过交易的扩散进一步加深对网络的理解。

之前我们讲过，区块链网络不生产交易，而只是交易的搬运工。从区块链网络示意图中可以看到，在区块链网络外围有大量的手机、电脑、汽车等外联设备，这些设备与任意的区块链节点连接，就能从该节点获取与自身相关的信息，诸如余额、历史交易等等。

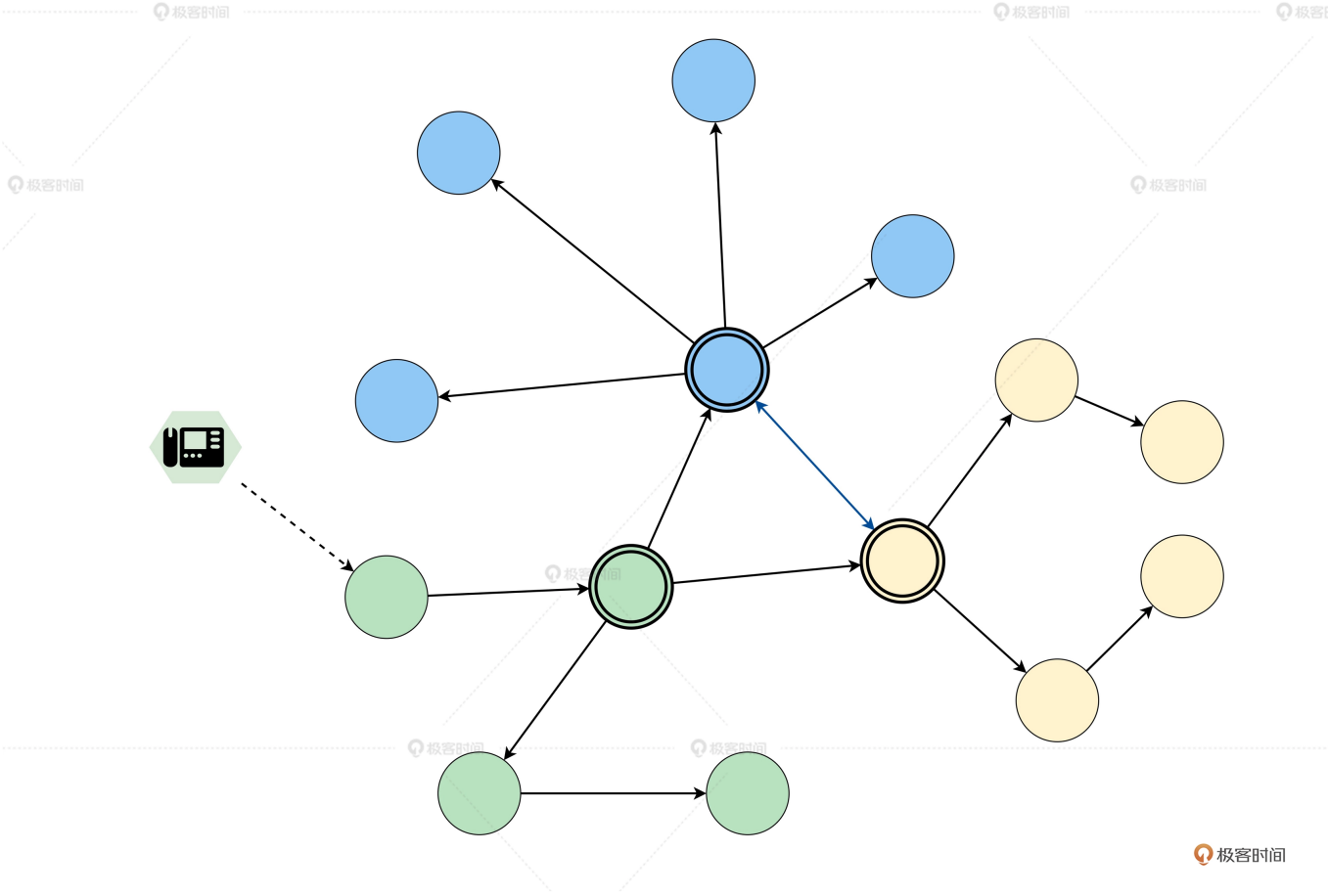
同时，外联设备所构建的交易会随之发送到与之相连的节点，所以它们是区块链网络的交易源头。



区块链网络示意图

那么外联设备将交易发送至某一区块链节点之后，交易在区块链网络中又是如何扩散的呢？

后面这张简化区块链网络示意图，可以让你直观感受一下这个扩散路径，这里需要着重观察**箭头的指向**。



交易扩散示意图

我先帮你理一下交易扩散的通用逻辑，当交易被发送至连接节点后，节点随后就将交易发送到了和它连接的、相邻的其他节点，其他节点依次将交易扩散给其连接的节点，而最终会有一个时刻，所有的节点都会收到该交易。

这非常类似于我们传递八卦的场景，一个朋友给你透露了一点小秘密，你没把持住告诉了其他朋友，然后一传十，十传百，最终你们这个小圈子基本上都知道了这个小秘密，是不是非常形象？所以这种模式我们也很生动地起名为八卦（Gossip）协议。

理解这种传播过程是相对容易的，但是我们应该注意到**不同网络拓扑对重复接收相同交易处理上的差别**。

以太坊网络的节点只与自己最近距离的相邻节点连接，交易的扩散并不存在回路的可能性，它的扩散路径更像是一种单向的持续向外广播，就像水永远只向低处流一样，交易会逐渐远离最初的节点，交易扩散效率较高。

而比特币的交易扩散对此的处理则有所不同。它的网络拓扑是随机的，交易扩散的时候是扩散至与之连接的节点，但扩散前并不知道对方是否已经接收过相同的交易，因此网络扩

散的效率是较低的。

随着网络节点规模的扩大，节点间连接关系更为无序，大量的网络带宽浪费在对交易的重复扩散中。节点接收到重复交易并不会再次理会，而是直接丢弃，白白做了无用功。你看，比特币的网络拓扑虽然结构简单，但也为此付出了代价。

对区块的扩散也遵循交易扩散的通用逻辑，只不过此时并不需要外联设备的参与，而是由首先满足共识条件的矿工节点发出，你可以先留下一个印象，等下一讲我们学共识算法的时候，我再详细讲解。

总结

点对点网络是区块链中最常用的网络交互模型，相比于中心架构的客户端服务器模型，每个节点具有对等的权利与义务，与区块链的去中心化特性相得益彰。

但点对点网络节点发现机制比中心化网络复杂得多，对此处理的不同衍生出中心、随机、混合及结构化等不同的网络拓扑结构。不同区块链有不同的选择，影响了区块链网络对交易及区块扩散处理上的不同。

其实，区块链中是先有去中心化思想还是先有点对点网络的启蒙，这个问题其实不是最重要的。讨论这个问题，是因为研究二者的关系可以让你更深刻地理解区块链网络。而在最后，我也想给出我的观点倾向，我认为是点对点网络的思想启发了中本聪，让他想到利用其无绝对中心的特性去构建去除第三方中介的数字货币系统。

1.区块链追求“摆脱中间商”的去中心化，即去除中心节点束缚。如同现在人人都有麦克风，区块链的每个节点也拥有同等权利和义务。

2.区块链网络一直处在中心化与绝对去中心化的动态平衡中。

3.因为节点发现机制的不同处理，点对点网络衍生出不同的网络拓扑结构。

说透区块链

赵铭 | 区块链服务平台资深架构师

识别二维码
免费试读

讨论

区块链技术到底是因为需要去中心化特性所以选择点对点网络，还是因为点对点网络的启发区块链才有的去中心化特性，你是如何看待二者间的因果关系呢？

扩展阅读

分布式哈希表的知识我并没有展开，但是你可以通过DHT 分布式哈希表以及死磕以太坊源码分析之 Kademlia 算法这两篇文章了解其原理，在我看来里面写的内容也相当精彩。

欢迎你在留言区跟我互动，主动思考、积极交流会让你更有收获。如果这一讲对你有帮助，也欢迎你分享给自己的朋友、同事。

分享给需要的人，Ta订阅后你可得 20 元现金奖励

赞 1 提建议

© 版权归极客邦科技所有，未经许可不得传播售卖。 页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 05 | 密码学：为什么说区块链站在了巨人肩膀上？

下一篇 07 | 共识（上）：拜占廷将军也讲少数服从多数？

更多课程推荐

精选留言 (4)

写留言

哄哄
2021-08-02

我觉得是点对点成熟的基础结构才有了去中心化的想法，正如密码学之于比特币

作者回复: 恩，与我的观点一致。区块链不仅是实现上四种基础技术的融合，思想也是深受启发

1

童言
2021-08-02

这一讲的内容让我回忆起了计算机网络的知识。交易扩散的步骤有点类似于计算机网络路由表的形成。

我个人感觉是先有区块链去中心化的需求，才会有技术选型上的点对点网络，毕竟技术一直都在，需求才是第一生产力。

展开

作者回复: 从这个角度看，确实也可以说的通。而且如果是这样，那中本聪的厉害程度又上升了一个台阶，勇于打破常规

1

静静聆听
2021-08-05

老师，可以加重一些对联盟链的介绍么，因为现在国内联盟链应该是发展重点

作者回复: 你好，你主要想看哪方面啊？课程主要介绍的是共性吧，但是会穿插一些差异

高鹏0409
2021-08-04

评论区里也是大神云集，看完原文一定要看评论

展开

编辑回复: 谢谢鼓励，后面内容更精彩~